# Practical No 7

**Aim:** Analyse the packet provided in lab and solve the questions using Wireshark

**-What web server software is used by** [**www.snopes.com?**](http://www.snopes.com/)

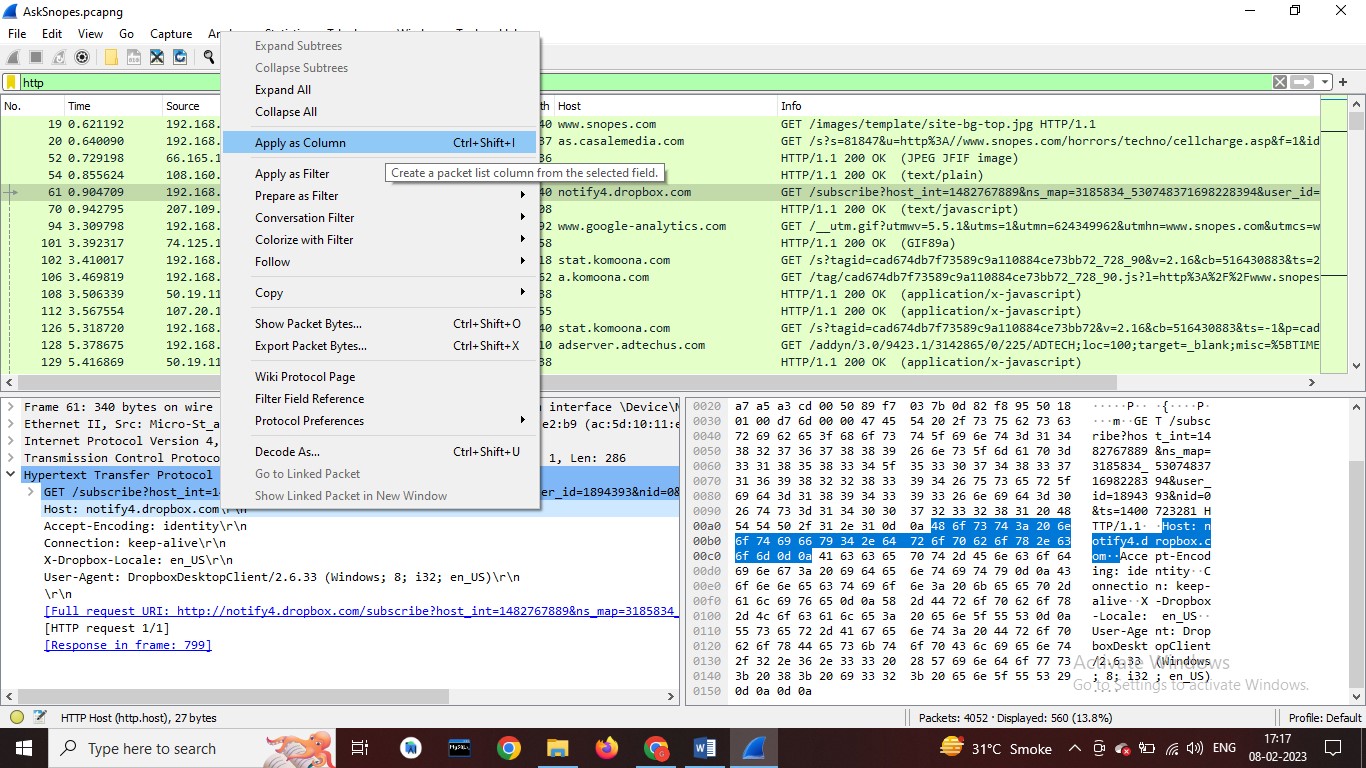
**-About what cell phone problem is the client concerned?**

**-According to Zillow, what instrument will Ryan learn to play? -How many web servers are running Apache?**

**-What hosts (IP addresses) think that jokes are more entertaining when they are explained?**

# Steps:-

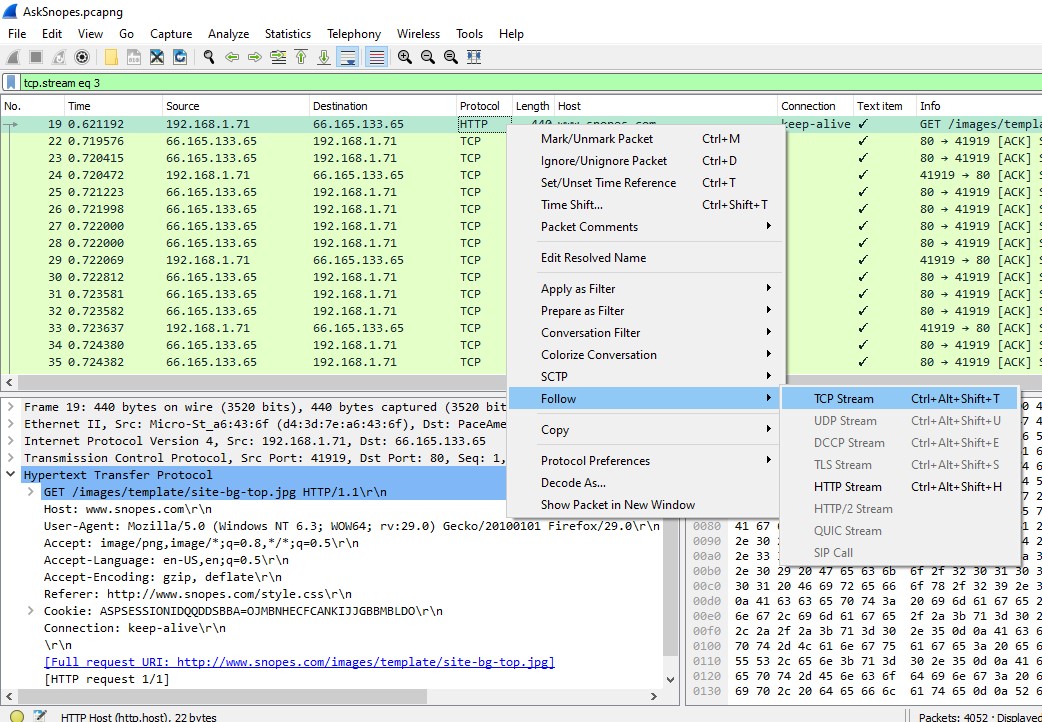
1. **What web server software is used by** [**www.snopes.com**](http://www.snopes.com/)  Analysis – The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then apply as Column.



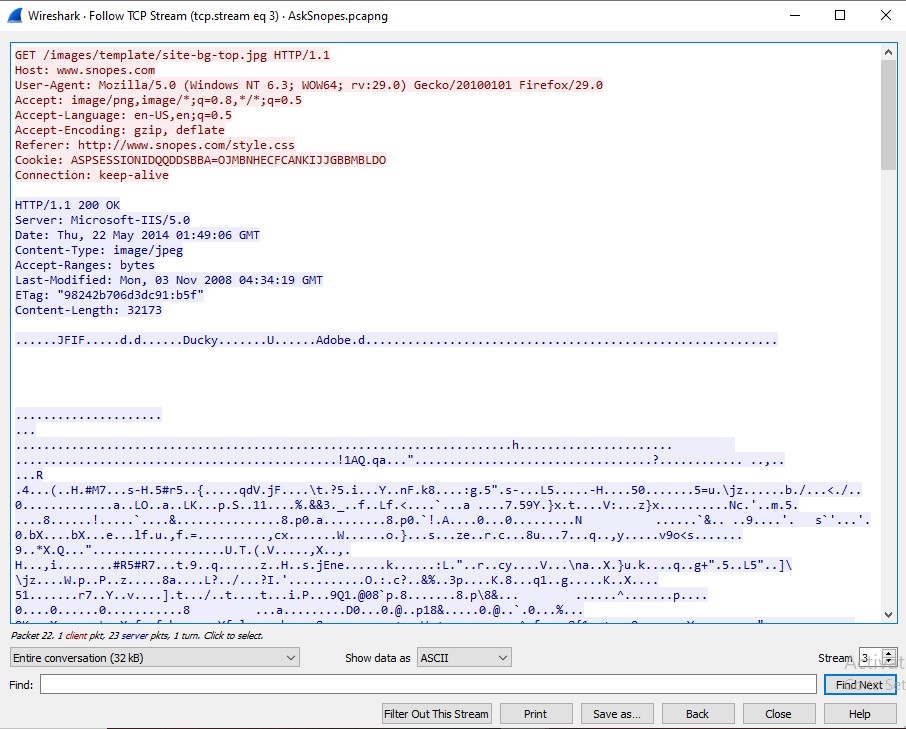
Now we can see our host [www.snopes.com](http://www.snopes.com/) in host column.



Click any of the http packet > right click> Follow> TCP Stream

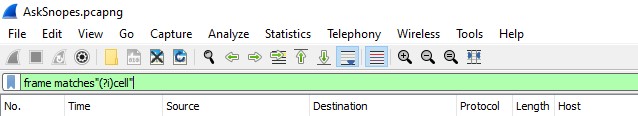


The webserver is Microsoft IIS/5.0

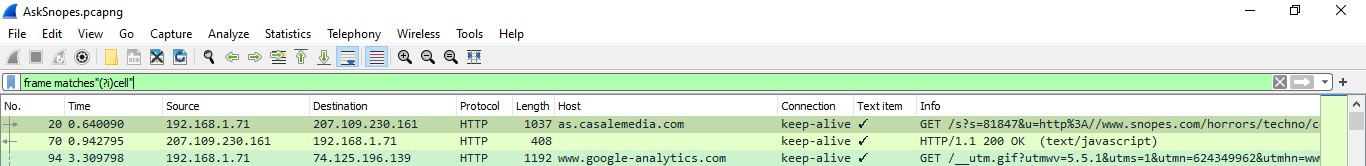


1. **About what cell phone problem is the client concerned?**

Analysis – Client talking about cell so we search for cell keyword in whole packets. We will use regular express for searching the cell keyword. Apply frame matches “(?!) cell”



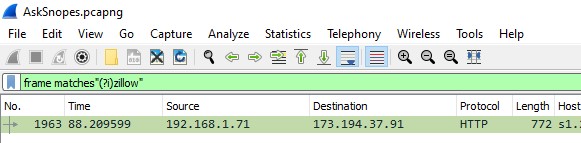
After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request cell keyword is in URL and it was about cell phone charging issue.



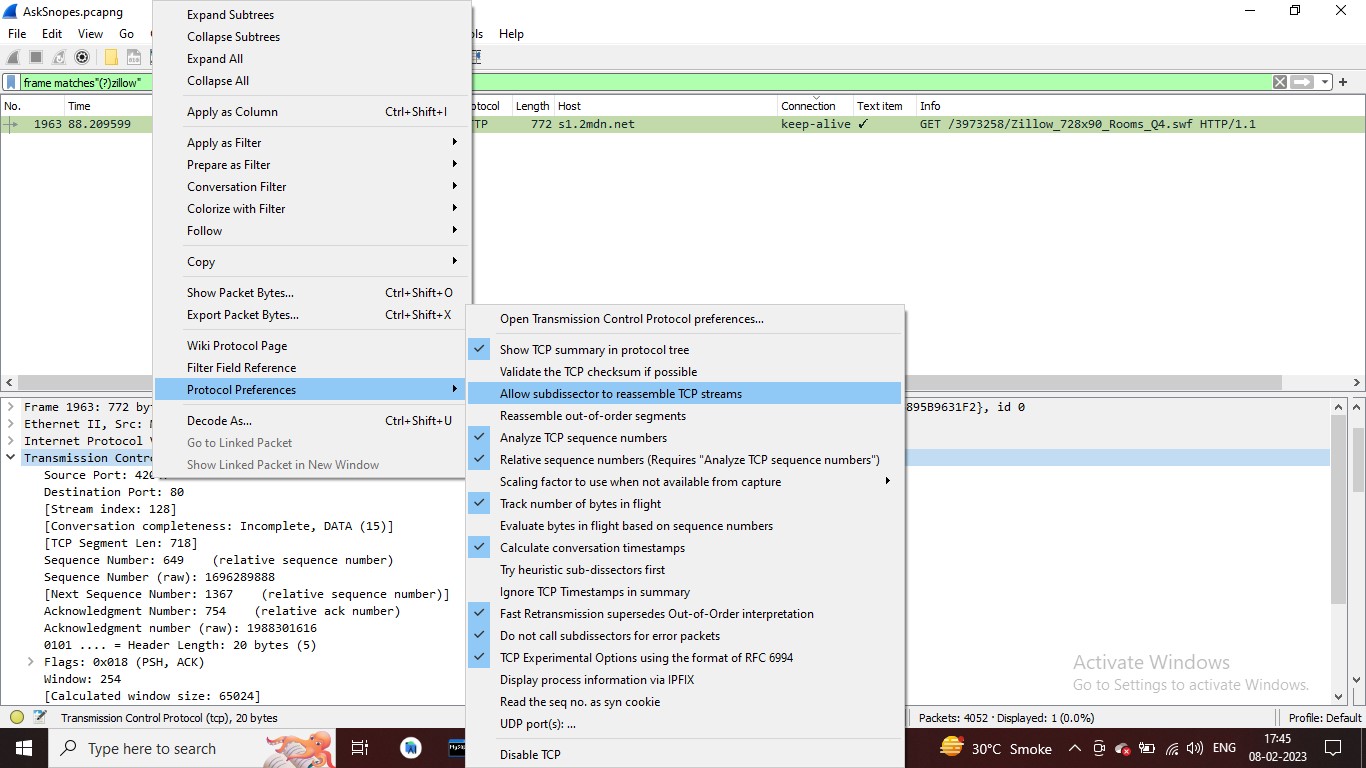
The Client concerns the cell charge.

1. **According to Zillow, what instrument will Ryan learn to play?**

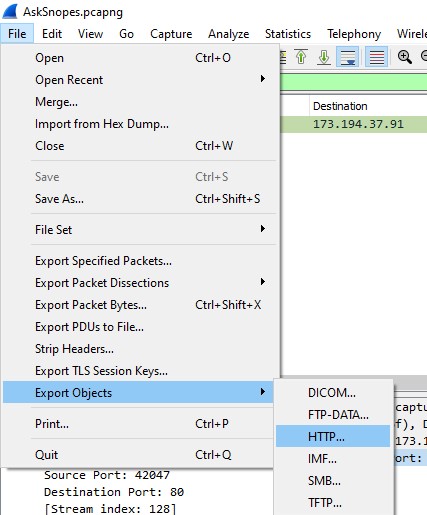
Analysis – As we did in the last challenge, we will apply a regular express filter for the Zillow keyword. Apply frame matched “(?!) zillow”



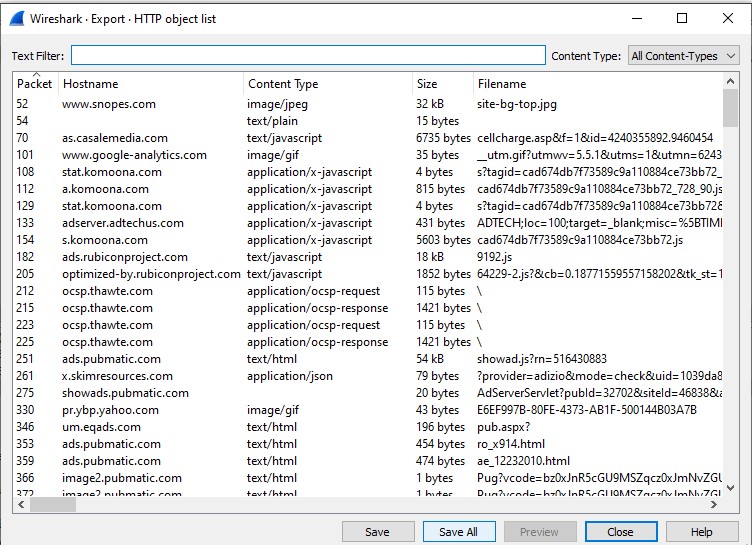
Select the packet and expand the Hypertext Transfer Protocol tab right click on it go to Protocol Preferences and check Allow subdissector to resemble TCP stream.



Now go to file and select Export Objects > HTTP. It will save all objects from the packet.

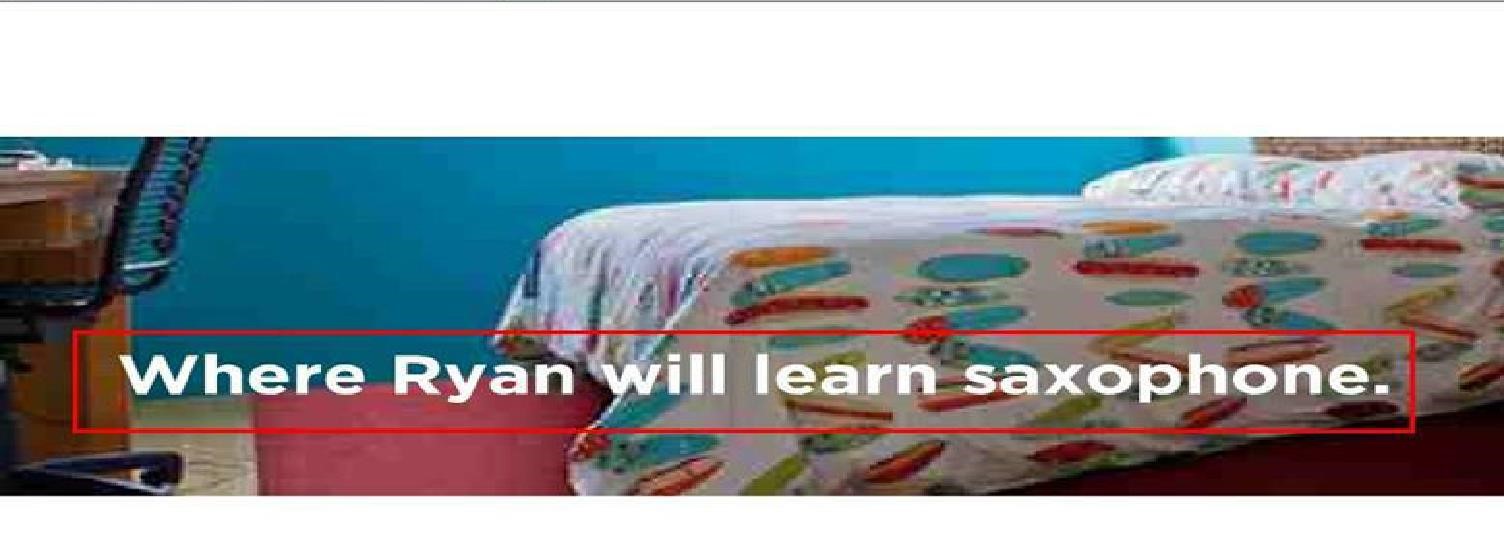


Click on Save all.



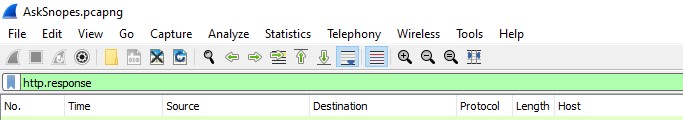
After saving all files in a directory and we found a swf file with name Zillow.

After opening the flash file, we saw that Zillow was trying to learn saxophone.

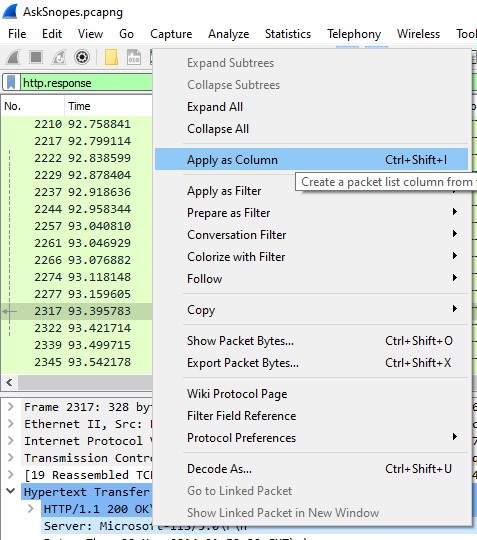


1. **How many web servers are running Apache?**

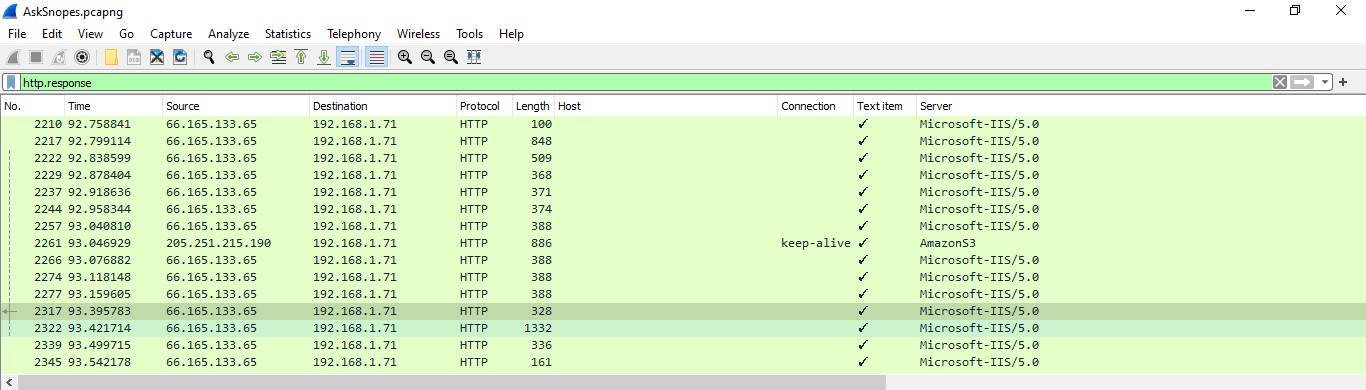
Analysis – The web server name can be retrieved from HTTP response header. So will apply filter http. response and we can see all http response packets.



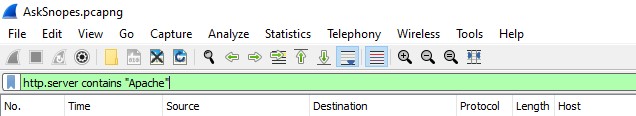
Now we will set the server header as column select any packet and right click on it then select Apply as Column.



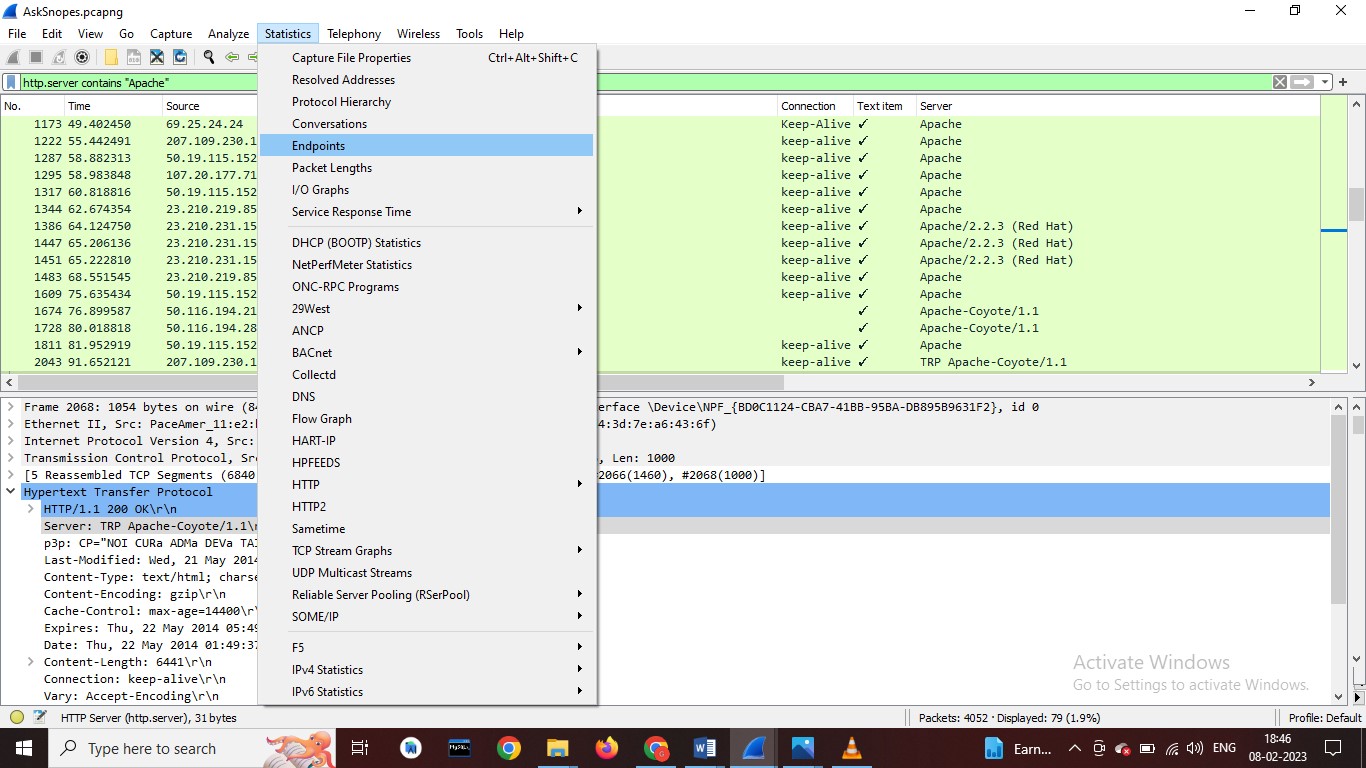
Now can see the server column where all server name is showing.



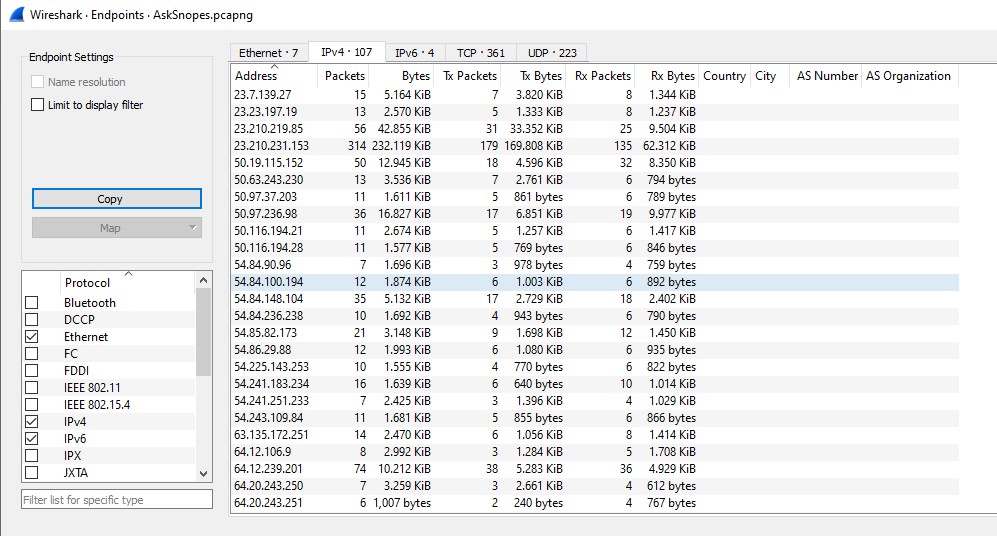
Now we have to check how many Apache packets are there we can’t count manually for each packet so we will apply another filter http.server contains “Apache”



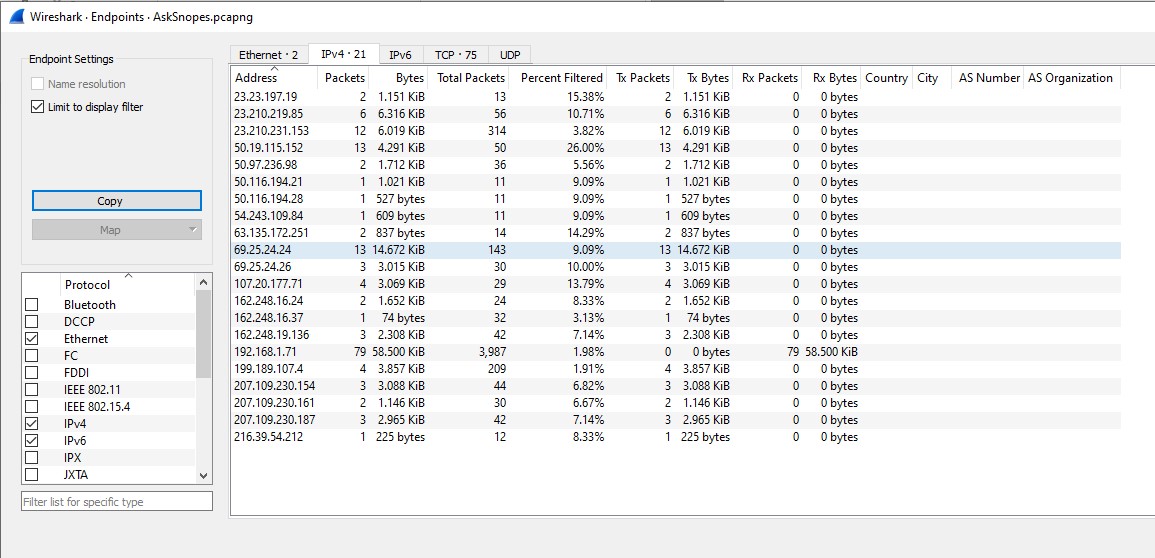
After applying filter go to Statistics > Endpoints



It will show all connections

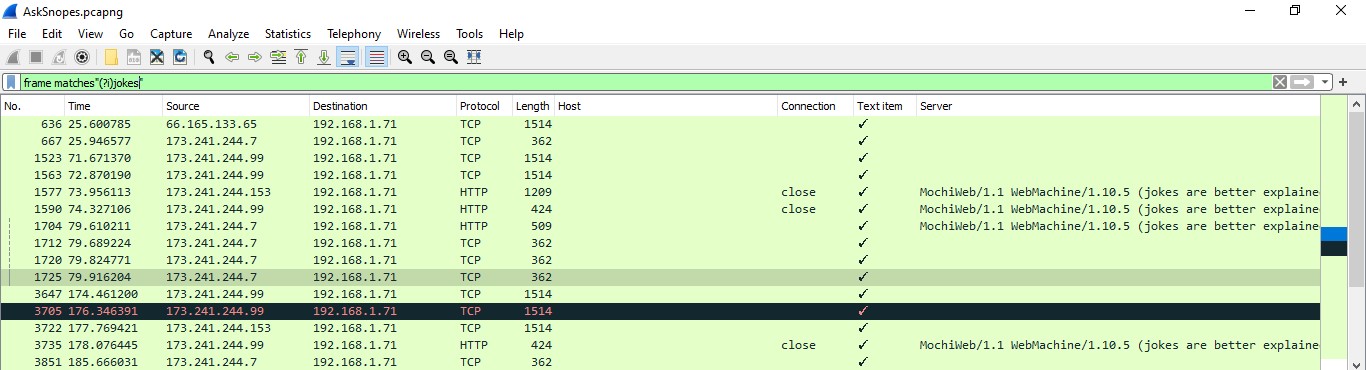
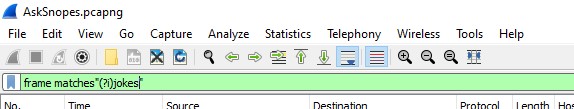


Check the limit to display filter then it will show the actual Apache connections. Now there are showing 22 connections but will exclude 192.168.1.71 because it is client’s IP not a server IP so there are actual 21 Apache servers.



**5] What hosts (IP addresses) think that jokes are more entertaining when they are explained**

Analysis – as we did last time we will apply filter, frame matches”(?!)jokes”



We have successfully analyzed the packets provided and solved the questions using wireshark.